## 日 本 国 特 許 庁 02.12.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2003年11月28日

出願番号

特願2003-399968

Application Number: [ST. 10/C]:

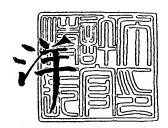
[ ] P 2 0 0 3 - 3 9 9 9 6 8 ]

出 願 人
Applicant(s):

松下電器産業株式会社

特許庁長官 Commissioner, Japan Patent Office 2005年 1月13日

シュリ



BEST AVAILABLE COPY

特許願 【書類名】 2048150054 【整理番号】 平成15年11月28日 【提出日】 特許庁長官 殿 【あて先】 G09C 1/00 【国際特許分類】 【発明者】 大阪府門真市大字門真1006番地 松下電器産業株式会社内 【住所又は居所】 【氏名】 中野 稔久 【発明者】 東京都江東区青梅2-79 東京国際交流館A0909 【住所又は居所】 ナッタポン アッタラパドゥン 【氏名】 【発明者】 東京都三鷹市大沢2-20-31-1-402 【住所又は居所】 古原 和邦 【氏名】 【発明者】 【住所又は居所】 神奈川県横浜市戸塚品濃町557-44-205 今井 秀樹 【氏名】 【特許出願人】 【識別番号】 000005821 【氏名又は名称】 松下電器產業株式会社 【代理人】 【識別番号】 100090446 【弁理士】 【氏名又は名称】 中島 司朗 【手数料の表示】 【予納台帳番号】 014823 21,000円 【納付金額】 【提出物件の目録】 【物件名】 特許請求の範囲 1 【物件名】 明細書 1 【物件名】 図面 1 【物件名】 要約書 1

9003742

【包括委任状番号】

#### 【書類名】特許請求の範囲

#### 【請求項1】

特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置と、前記無効化情報を記録する記録媒体と、前記記録媒体から前記無効化情報を読み出して処理する端末装置からなる著作権保護システムであって、

前記鍵管理装置は、

前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、

前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と

前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする著作権保護システム。

#### 【請求項2】

前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする請求項1記載の著作権保護システム。

#### 【請求項3】

前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分 集合の鍵を生成することを特徴とする請求項1記載の著作権保護システム。

#### 【請求項4】

前記鍵管理装置はさらに、前記部分集合と割り当てた鍵の対応関係、並びに生成された 鍵の相互関係を記憶する記憶部を備えることを特徴とする請求項1記載の著作権保護シス テム。

#### 【請求項5】

前記鍵管理装置の記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前期テーブルを記憶することを特徴とする請求4記載の著作権保護システム。

#### 【請求項6】

前記鍵管理装置はさらに、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、

前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を 選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵 から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれ る最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布すること を特徴とする請求項1記載の著作権保護システム。

#### 【請求項7】

前記鍵管理装置の無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合 を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端 末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が 何れかの部分集合に含まれるまで繰り返し行うことを特徴とする請求項1記載の著作権保 護システム。

#### 【請求項8】

前記端末装置はさらに、前記無効化情報を処理する鍵を格納する格納部を備え、 前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴と する請求項1記載の著作権保護システム。

#### 【請求項の】

前記端末装置の格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納すること を特徴とする請求項8記載の著作権保護システム。

#### 【請求項10】

前記端末装置の格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が

生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする請求項8記載の著作権 保護システム。

#### 【請求項11】

前記端末装置はさらに、前記格納部に格納する鍵から、他の部分集合に割り当てられた 鍵を生成する鍵生成部を備え、

前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から他の部分集合に割り当てられた鍵を生成することを特徴とする請求項10記載の著作権保護システム。

#### 【請求項12】

前記端末装置はさらに、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする請求項1記載の著作権保護システム。

#### 【請求項13】

前記端末装置はさらに、前記記録媒体から暗号化されたコンテンツを読み出して復号、 及び再生する再生部を備えることを特徴とする請求項1記載の著作権保護システム。

#### 【請求項14】

前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されることを特徴とする請求項1記載の著作権保護システム。

#### 【請求項15】

前記記録媒体の代わりに通信媒体を利用することを特徴とする請求項1記載の著作権保 護システム。

#### 【請求項16】

特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置であって、 前記鍵管理装置は、

前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、 前記部分集合に対して鍵を割り当てる割当部と、

前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と

前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする鍵管理装置。

#### 【請求項17】

前記鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする請求項16記載の鍵管理装置。

#### 【請求項18】

前記鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とする請求項16記載の鍵管理装置。

#### 【請求項19】

前記鍵管理装置はさらに、

前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする請求項16記載の鍵管理装置。

#### 【請求項20】

前記記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前期テーブルを記憶することを特徴とする請求19記載の鍵管理装置。

#### 【請求項21】

前記鍵管理装置はさらに、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、

前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を 選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵 から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれ る最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布すること を特徴とする請求項16記載の鍵管理装置。

#### 【請求項22】

前記無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、 前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが 含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分 集合に含まれるまで繰り返し行うことを特徴とする請求項16記載の鍵管理装置。

#### 【請求項23】

記録媒体から無効化情報を読み出して処理する端末装置であって、

前記端末装置は、前記無効化情報を処理する鍵を格納する格納部を備え、

前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴とする端末装置。

#### 【請求項24】

前記格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする請求項23記載の端末装置。

#### 【請求項25】

前記格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする請求項23記載の端末装置。

#### 【請求項26】

前記端末装置はさらに、前記格納部に格納する鍵から、他の部分集合に割り当てられた 鍵を生成する鍵生成部を備え、

前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から他の部 分集合に割り当てられた鍵を生成することを特徴とする請求項25記載の端末装置。

#### 【請求項27】

前記端末装置はさらに、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする請求項23記載の端末装置。

#### 【請求項28】

前記端末装置はさらに、前記記録媒体から暗号化されたコンテンツを読み出して復号、 及び再生する再生部を備えることを特徴とする請求項23記載の端末装置。

#### 【請求項29】

特定の装置を無効化するための無効化情報を記録する記録媒体であって、

鍵管理装置は、著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備え、

前記鍵管理装置により生成された無効化情報を記録することを特徴とする記録媒体。

#### 【請求項30】

前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのか を示す情報が付与されており、前記付与された情報と共に前記鍵無効化情報を記録するこ とを特徴とする請求項29記載の記録媒体。



【発明の名称】著作権保護システム、鍵管理装置、端末装置、及び記録媒体 【技術分野】

#### [0001]

本発明は、映画や音楽などの著作物であるコンテンツのデジタル化データを、光ディスク等の大容量記録媒体に記録、あるいは再生するシステムに関し、特に不正装置を使ったコンテンツの記録、あるいは再生による著作権侵害を防止するために、不正装置が持つ鍵では、コンテンツの記録、あるいは再生に必要な鍵が算出できず、不正装置以外の正規装置では、いずれの装置においても共通の鍵が算出できるような著作権保護システムに関する。

#### 【背景技術】

#### [0002]

近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、 音声等からなるデジタルコンテンツ(以下、コンテンツ)を生成して、光ディスク等の大 容量記録媒体に格納して配布する、あるいはネットワークや放送を介して配信するシステ ムが現れている。

配信されたコンテンツは、コンピュータや再生装置等で読み出されて、再生、あるいはコピーの対象となる。

#### [0003]

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピーといった不正利用を防止するために暗号化技術が用いられる。

具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号化鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号して、コンテンツの再生等を行うことができる、というものである。なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法等がある。

#### [0004]

このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析において、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する記録装置、再生装置、あるいはソフトウェアを作成し、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを鍵無効化技術と呼び、鍵無効化を実現するシステムとして、木構造と呼ばれる階層構造を利用した鍵無効化技術が、特許文献1、及び非特許文献1に開示されている。

#### [0005]

以下、非特許文献1に記載されている従来の鍵無効化技術について説明する。

まず、「Subset Difference」(以降、差分集合と呼ぶ)についての定義を行う。差分集合は、大きな木構造の集合から、それよりも小さな木構造の集合を取り除いたときの、各装置(リーフ)からなる集合と定義する。大きな木構造のルートと小さな木構造のルートの2つを定めることにより、差分集合は決定される。そして、各差分集合に対してそれぞれ復号鍵が割り当てられる。

#### [0006]

さらに、コンテンツはコンテンツ鍵で暗号化されており、各装置は復号鍵を保持し、各装置が自身の保持する復号鍵を用いてコンテンツ鍵を求める際に必要とされるデータを鍵データと呼ぶ。一般的に、鍵データはコンテンツ共に配信され、コンテンツの配信に記録媒体を利用する場合は、鍵データは記録媒体に記録される。

無効化されない装置の集合を、差分集合でカバーすることによって、鍵データのサイズ を削減することが可能となる。図15にその概念図を示す。図15において、大きな木構 造のルートをVi、小さな木構造のルートをVjとした場合、印をつけた2つのリーフに 割り当てられた装置を無効化する集合は、Viをルートとする木構造からViをルートと する木構造を取り除いた差分集合Si.iとなる。さらに、必要となる鍵データは、前記 差分集合Si, jに対応した1つの暗号化鍵Li, jを用いて暗号化された、1つの暗号 化コンテンツ鍵となる。

#### [0007]

また、別の例として、装置数16の木構造において、装置3、装置4、装置13、装置 15が無効化されている場合の差分集合、並びにコンテンツ鍵を暗号化するための暗号化 鍵Si,jを図16に示す。例えば、装置9~装置12は、V3をルートとする木構造か ら、V7をルートとする木構造を取り除いた差分集合S3,7に属する。図16おいては 、同一の差分集合Si,jに属する装置は、共通の復号鍵を保持している。例えば、差分 集合S2,9に属する装置1、装置2、装置5~装置8は、共通の復号鍵L2,9を保持 し、差分集合S3,7に属する装置9~装置12は、共通の復号鍵L3,7を保持してい る。さらに、コンテンツ鍵は、L2, 9、L3, 7、L14, 28、L15, 31でそれ ぞれ暗号化されるため、いずれの復号鍵も保持していない装置3、装置4、装置13、装 置15は、コンテンツ鍵を復号することができず、コンテンツを扱うことができない。

#### [0008]

ここで、各装置は、無効化される装置の位置関係に応じた復号鍵を保持する必要があり 、その基本的な考え方は次の通りである。ある装置が差分集合Si,jに対応した復号鍵 Li, jを保持する場合、その装置は、差分集合Si, kに対応した復号鍵Li, kも保 持する。ただし、VkはVjの部分集合とする。このとき、Li,kは、Li,jから計 算で求めることができるようにするが、その逆は計算では求められないようにするため一 方向性関数を利用する。

#### [0009]

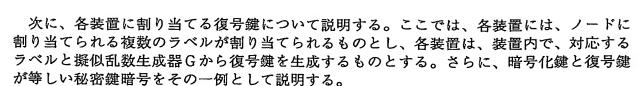
まず、木構造の各ノードに割り当てられる暗号化鍵(この暗号化鍵は、各装置が保持す る復号鍵と対応する)について、図17に示す2分木の木構造の例を用いて説明する。

図17に示す木構造の各ノードには、それぞれ個別のTビットの「ラベルーと呼ばれる 識別子が付与されている。そして、入力データ長Tビットに対して、3Tビットの乱数を 生成する擬似乱数生成器Gを用意する。ラベルA1を擬似乱数生成器Gの入力とした場合 に、出力される3Tビットのうち、前半TビットをラベルA1の左下の子のラベルとし、 真ん中のTビットをラベルA1のノードに対応する暗号化鍵とし、後半Tビットをラベル Alの右下の子のラベルとし、それぞれをAlL、AlM、AlRと表現する。図17で は、各ノードには予めラベルA1、A2、A3、A4等が個別に割り当てられており、加 えて上位のラベルから派生してきた新たなラベルが追加される。例えば、上から3層目の ノード4001においては、当該ノードに予め割り当てられたラベルA4に加え、上位の ラベルA1から派生したラベルA1LL、並びに同じく上位のラベルA2から派生したラ ベルA2Lと計3個のラベルが割り当てられことになる。さらに、各ノードに割り当てら れる暗号化鍵の数は、当該ノードに割り当てられたラベルの数と等しくなるため、ノード 4001には、A1LLM、A2LM、A4Mの計3つの暗号化鍵が割り当てられること になる。

#### [0010]

ここで、差分集合Si,iに対応する暗号化鍵Li,iと、上記各ノードに割り当てら れた暗号化鍵の関係を示す。ノードViとノードVjを決定した場合、差分集合Si,j に対応する暗号化鍵Li、iは、ノードViに割り当てられたラベルから派生したラベル のうち、ノードVjに追加されたラベルに対応する暗号化鍵となる。図17の例において 、ノードViのラベルをA1、ノードViのラベルをA4とすると、暗号化鍵Li.iは A1LLMとなる。

#### [0011]



具体的には、各装置が割り当てられたリーフから、ルートに至る経路上に存在するノードにぶら下がるノードに着目して、当該ノードに割り当てられているラベルが、各装置に対して割り当てられる。その具体例を図18に示す。

#### [0012]

図18は、装置の総数を8台としたときの、各装置に割り当てられるラベルを示している。装置1に割り当てられるラベルは、装置1からルートに至る経路上に存在するノードA、ノードB、ノードDにそれぞれぶら下がるノードC、ノードE、及び装置2が割り当てられるリーフのラベルである。図18に示す通り、各装置に対しては該当するラベルが全て割り当てられる。このとき、各装置に割り当てられるラベルの総数は、装置の総数を t台とした場合、 $0.5(\log_2 t)^2+0.5\log_2 t$  個である。これは、各装置に割り当てられるラベルの数が、2層目に1個、3層目に2個、…、最下位層に $\log_2 t$  個であることから、 $1+2+\cdots+\log_2 t=0.5(\log_2 t)^2+0.5\log_2 t$  となるからである。

#### [0013]

次に、図18を用いて、実際に装置を無効化する場合の例を説明する。

(1)何れの装置も無効化されていない初期状態では、ラベルAL、ARに対応する鍵ALM、及びARMを用いてコンテンツ鍵を暗号化する。全ての装置は、ラベルAL、あるいはラベルARを保持しており、それらから、復号鍵ALM、あるいはARMを生成することができる。従って、生成した復号鍵でコンテンツ鍵を復号することができ、さらには、復号したコンテンツ鍵を利用してコンテンツを復号することができる。

#### [0014]

(2)装置1がハックされて、保持する全ての鍵が暴露された場合は、ラベルAとラベルALLLを指定して、ラベルAをルートとする大きな木構造から、ラベルALLLの小さいな木構造(リーフ)を取り除く。そして、ラベルALLLに対応する暗号化鍵ALLLMを用いてコンテンツ鍵を暗号化する。装置2は、ラベルALLLから復号鍵ALLLMを生成することができ、装置3、装置4は、ラベルALLから復号鍵ALLLMを生成することができ、さらに、装置5~装置8は、ラベルALから復号鍵ALLLMを生成することができる。装置1は、擬似乱数生成器Gが一方向性であることから、自身が保持するラベルからは復号鍵ALLLMを生成することができない。

#### [0015]

最後に、非特許文献1に示す従来の鍵無効化技術においては、装置数が約10億台(高さ30の2分木)のシステムを考えた場合、各装置が保持する鍵の数は465個となる。

【特許文献1】特開2002-281013号公報

【非特許文献 1 】 D. Naor, M. Naor, and J. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers", Proceedings of CRYPTO2001, LNCS2139, pp.41-62, 2001.

#### 【発明の開示】

【発明が解決しようとする課題】

#### [0016]

しかしながら、非特許文献1に開示されている従来の鍵無効化技術では、各装置が内蔵 する鍵の数が膨大になるという課題がある。

本発明は、前記従来の課題を解決するためのもので、各装置が内蔵する鍵の数を削減可能な鍵無効化システムの提供を目的とする。

#### 【課題を解決するための手段】

#### [0017]

本発明は、特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置



と、前記無効化情報を記録する記録媒体と、前記記録媒体から前記無効化情報を読み出して処理する端末装置からなる著作権保護システムであって、前記鍵管理装置は、前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする。

#### [0018]

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の鍵生成部は、前 記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とす る。

#### [0019]

また、本発明は、前記著作権保護システムであって、前記鍵管理装置は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の記憶部は、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前期テーブルを記憶することを特徴とする。

#### [0020]

また、本発明は、前記著作権保護システムであって、前記鍵管理装置は、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれる最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布することを特徴とする。

#### [0021]

また、本発明は、前記著作権保護システムであって、前記鍵管理装置の無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分集合に含まれるまで繰り返し行うことを特徴とする。

#### [0022]

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記無効化情報 を処理する鍵を格納する格納部を備え、前記格納部には、自身が含まれる部分集合に割り 当てられた鍵を格納することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置の格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする。

#### [0023]

また、本発明は、前記著作権保護システムであって、前記端末装置の格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記格納部に格納する鍵から、他の部分集合に割り当てられた鍵を生成する鍵生成部を備え、前記鍵生成部は、部分集合と鍵の対応関係、並びに生成された鍵の相互関係から他の部分集合に割り当てられた鍵を生成することを特徴とする。

#### [0024]

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする。



また、本発明は、前記著作権保護システムであって、前記端末装置は、前記記録媒体から暗号化されたコンテンツを読み出して復号、及び再生する再生部を備えることを特徴とする。

#### [0025]

また、本発明は、前記著作権保護システムであって、前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されることを特徴とする。

また、本発明は、前記著作権保護システムであって、前記記録媒体の代わりに通信媒体を利用することを特徴とする。

#### [0026]

また、本発明は、特定の装置を無効化するための無効化情報の生成を行い配布する鍵管理装置であって、前記鍵管理装置は、前記著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備えることを特徴とする。

#### [0027]

また、本発明は、前記鍵管理装置であって、前記鍵生成部は、前記部分集合に割り当てられた鍵から、一方向性関数を利用して他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記鍵生成部は、前記部分集合に割り当てられた鍵から、複数の他の部分集合の鍵を生成することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記部分集合と割り当てた鍵の対応関係、並びに生成された鍵の相互関係を記憶する記憶部を備えることを特徴とする。

#### [0028]

また、本発明は、前記鍵管理装置であって、前記記憶部は、前記部分集合と割り当てた 鍵の対応関係、並びに生成された鍵の相互関係を、テーブルを利用して管理し、前期テー ブルを記憶することを特徴とする。

また、本発明は、前記鍵管理装置であって、前記部分集合に対して割り当てた鍵を前記端末装置に配布する鍵配布部を備え、前記鍵配布部は、鍵を配布する端末装置が含まれる部分集合のうち、最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布し、さらに、前記配布した鍵から生成される鍵が割り当てられた部分集合を除く部分集合から、前記端末装置が含まれる最小の部分集合を選択して、前記選択した部分集合に割り当てられた鍵を配布することを特徴とする。

#### [0029]

また、本発明は、前記鍵管理装置であって、前記無効化情報生成部は、有効な端末装置だけが含まれる最大の部分集合を選択して、前記選択した部分集合に含まれない端末装置に対しては、さらに、それら端末装置だけが含まれる最大の部分集合を選択して、前記選択を、全ての有効な端末装置が何れかの部分集合に含まれるまで繰り返し行うことを特徴とする。

#### [0030]

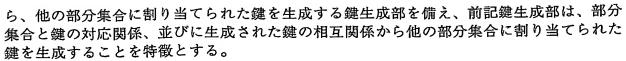
また、本発明は、記録媒体から無効化情報を読み出して処理する端末装置であって、前記端末装置は、前記無効化情報を処理する鍵を格納する格納部を備え、前記格納部には、自身が含まれる部分集合に割り当てられた鍵を格納することを特徴とする。

また、本発明は、前記端末装置であって、前記格納部は、鍵と部分集合の対応関係を示す情報も合わせて格納することを特徴とする。

#### [0031]

また、本発明は、前記端末装置であって、前記格納部は、ある部分集合に割り当てられた鍵から、他の部分集合の鍵が生成可能な場合、前記生成可能な鍵は格納しないことを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記格納部に格納する鍵か



#### [0032]

また、本発明は、前記端末装置であって、前記端末装置は、前記記録媒体に対して、暗号化されたコンテンツを記録する記録部を備えることを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記記録媒体から暗号化されたコンテンツを読み出して復号、及び再生する再生部を備えることを特徴とする。

また、本発明は、特定の装置を無効化するための無効化情報を記録する記録媒体であって、鍵管理装置は、著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備え、前記鍵管理装置により生成された無効化情報を記録することを特徴とする。

#### [0033]

また、本発明は、前記記録媒体であって、前記鍵管理装置が生成した無効化情報には、どの部分集合の鍵に基づいて生成したのかを示す情報が付与されており、前記付与された情報と共に前記鍵無効化情報を記録することを特徴とする。

#### 【発明の効果】

#### [0034]

本発明によれば、各装置が内蔵する鍵の数を削減することが可能である、具体的には、木構造の高さをTとした場合、当該システムに属する1/2台の装置においてT-1個の鍵が削減され、1/4台の装置においてT-2個の鍵が削減され、 $1/(2^k)$ 台の装置においてT-k個の鍵が削減される。

#### 【発明を実施するための最良の形態】

#### [0035]

以下、本発明の実施の形態について、図面を用いて説明する。

図1は、本発明における著作権保護システムの概念図を示している。著作権保護システム1は、鍵管理装置100、記録装置110、記録媒体120、再生装置130からなる。鍵管理装置100は、記録装置110、並びに再生装置130に対してデバイス鍵を発行し、デバイス鍵は各装置の内部に格納される。また、鍵管理装置100は、記録媒体120に記録される。記録装置110は、記録媒体120が挿入された場合、記録媒体120から鍵無効化データを読み出し、デバイス鍵を用いて処理することで、コンテンツの暗号化に利用する鍵を獲得することができる。そして、獲得した鍵に基づいてコンテンツを暗号化して、暗号化コンテンツを記録媒体120が挿入された場合、記録媒体120から鍵無効化データを読み出し、デバイス鍵を用いて処理することで、コンテンツが記録された記録媒体120が挿入された場合、記録媒体120から鍵無効化データを読み出し、デバイス鍵を用いて処理することで、暗号化コンテンツの復号に必要な鍵を獲得することができる。そして、獲得した鍵に基づいて暗号化コンテンツを復号して、コンテンツを再生する

#### [0036]

図2は、鍵管理装置100の構成要素を示している。鍵管理装置100は、木構造に対する各装置の割り当て状態、並びにデバイス鍵に関する情報を格納する鍵情報生成/格納部201と、鍵情報生成/格納部201に格納する情報から、記録装置110、並びに再生装置130に発行するデバイス鍵を選択して配布するデバイス鍵配布部202と、無効化すべき装置を特定する無効化装置特定部203と、鍵情報生成/格納部201に格納する情報、並びに無効化装置特定部203が特定した無効化装置に関する情報から、記録媒体120に記録する鍵無効化データを生成する鍵無効化データ生成部204を備える。また、鍵情報生成/格納部201は、図3に示すような木構造を利用して各装置を管理している。



図3は、2分木の木構造で装置の総数を8台とした場合の例を示している。木構造における各層をレイヤと呼び、レイヤ0のノードをルート、最下位レイヤ(図3の例では、レイヤ3)のノードをリーフと呼ぶ。また、各装置は、木構造のリーフに対して1対1に割り当てられる。

次に、鍵管理装置100が鍵情報生成/格納部201において、デバイス鍵の生成、及び管理を行う方法について説明する。ここでは、その一例として、テーブルを利用して、木構造のリーフに割り当てられた装置の部分集合と、デバイス鍵との対応関係を管理する方法についてその詳細を説明する。テーブルを作成する動作フローを図4に示す。

#### [0038]

- S401:木構造の高さをTとする。図3に示す木構造の例では、T=3である。
- S402:以下のS403からS408までの操作をi=0~Tまで繰り返し行う。
- S403: レイヤiに存在するノードの数をNとし、レイヤiに存在するノードをルートとした部分木の高さをHとする。図3に示す木構造の例では、i=1の場合、ノードの数N=2、部分木の高さH=2である。

#### [0039]

S404:以下のS405からS407までの操作をj=0~H-1まで繰り返し行う

S 4 0 5:以下のS 4 0 6の操作を k = 1~Nまで繰り返し行う。

S406:レイヤiの左からk番目のノードをルートとする部分木から、2~j個の装置だけを除いた装置の部分集合を生成する。そして、生成した部分集合を、テーブルのj+1行目の左から順に格納していく。ただし、複数の装置を除く場合は、除く装置全てが共通の親ノードを持つ場合のみとする。図3に示す木構造の例では、レイヤ0、左から1番目の木構造から2個(j=1)の端末を除く場合、共通の親ノードを持つ装置1、装置2を除くパターン、同じく共通の親ノードを持つ装置3、装置4を除くパターン、さらに共通の親ノードを持つ装置5、装置6を除くパターン、最後に共通の親ノードを持つ装置7、装置8を除くパターンの4パターンとなり、テーブルの2行目の左から順に格納する

#### [0040]

S407: k=k+1を計算してS405に戻る。

S408: j = j + 1を計算してS404に戻る。

S409: i = i + 1を計算してS402に戻る。

以上の操作により生成されたテーブルを図5に示す。テーブルの1行目501は、木構造全体(装置数8)の集合から、装置を1台だけ除いた場合の部分集合を示している。さらに、テーブルの2行目502は、同じく木構造全体の集合から、共通の親を持つ装置2台を除いた場合の部分集合を示し、3行目503は、共通の親を持つ装置4台を除いた場合の部分集合を示している。

#### [0041]

次に、生成したテーブルの各要素(部分集合)に対して、デバイス鍵を生成して割り当てる動作フローを図6に示す。ただし、デバイス鍵を示すKm、及びKm+1のmとm+1は、鍵が割り当てられる毎に1ずつ増加する値とする。

S601:木構造の高さをTとする。図3に示す木構造の例では、T=3である。

S602:以下のS603からS608までの操作をh=1~2 Tまで繰り返し行う

#### [0042]

 $S603: (T^2+T)/2$ 行、h列の部分集合に対してデバイス鍵Kmを割り当てる。図5に示すテーブルの例では、6行、1列の部分集合1に対して、まずデバイス鍵が割り当てられる。

S604:以下のS605からS607までの操作を $i = ((T^2+T)/2)-1$ ~1まで繰り返し行う。

#### [0043]

S605:i-1行目で鍵が割り当てられた部分集合の数をJとする。以下のS606の操作を $j=1\sim J$ まで繰り返し行う。

S606:i-1行目の鍵の割り当てられた部分集合Ajを基準として、テーブルのi行目を左から順に探索していき、部分集合Ajを含む部分集合を最大2つまで見つけ、最初の部分集合をBj、次の部分集合をCjとする。さらに、部分集合Ajに割り当てられたデバイス鍵を擬似乱数生成器の入力として、その出力Km、Km+1をそれぞれ部分集合Bj、Cjのデバイス鍵として割り当てる。

#### [0044]

 $S \cdot 6 \cdot 0 \cdot 7 : j = j + 1$ を計算して $S \cdot 6 \cdot 0 \cdot 5$ に戻る。

S608: i=i-1を計算してS604に戻る。

S609: h=h+1を計算してS603に戻る。

以上の操作により生成された、部分集合とデバイス鍵の対応テーブルを図 7 に示す。これは、1 行、1 列は、部分集合 1 2 3 4 5 6 7 に対してデバイス鍵 K 8 が割り当てられたことを意味し、1 行、2 列は、部分集合 1 2 3 4 5 6 8 に対してデバイス鍵 K 9 が割り当てられたことを意味する。

#### [0045]

また、デバイス鍵の相互関係を示すテーブルを図8に示す。これは、部分集合1に割り当てられたデバイス鍵から、擬似乱数生成器を利用して、部分集合12のデバイス鍵が生成され、さらに、部分集合12のデバイス鍵から、同じく擬似乱数生成器を利用して部分集合123、並びに部分集合124の鍵が生成されたこと意味する。図8より、部分集合1に割り当てられたデバイス鍵からは、擬似乱数生成器を利用することで、部分集合12、123、124、1234、123456、123478、12345676、1234568、12345676、1234568、1234578、12345678の全てのデバイス鍵が算出可能であることが分かる。

#### [0046]

次に、鍵管理装置100がデバイス鍵配布部202において、鍵情報生成/格納部20 1に格納するテーブルから、デバイス鍵を選択して、各装置に割り当てる動作フローを図 9に示す。

S901:デバイス鍵を与える装置の番号をnとする。

S902: テーブルの( $T^2+T$ )/2行、1列を起点として、テーブルの左から右、上から下の順でテーブルの全要素を探索する。ここで、テーブルの全要素をYとする。以下のS903の操作を $i=1\sim Y$ まで繰り返し行う。図7に示すテーブルの例では、Y=34である。

#### [0047]

S903:デバイス鍵を与える装置の番号nを含む部分集合に割り当てられている(削除されていない)デバイス鍵Kmを当該装置に与える。さらに、当該デバイス鍵から生成することが可能な全てのデバイス鍵をテーブルから削除する。

S904: i = i + 1を計算してS902に戻る。

以上の操作により与えられたデバイス鍵と装置の関係を図10に示す。装置1には、K1、K15、K23、K27の4つのデバイス鍵が与えられ、装置<math>2には、K12、K2、K16、K23、K28の5つのデバイス鍵が与えられる。各装置に対しては、図<math>10に示すテーブルの各行(部分集合とデバイス鍵の対応関係)と、図8に示した、デバイス鍵(部分集合)の相互関係を示すテーブルも一緒に与えられる。

#### [0048]

次に、鍵管理装置100が鍵無効化データ生成部204において、鍵無効化データを生成する動作について説明する。鍵無効化データ生成部204は、無効化装置特定部203が特定した装置番号を除く装置のうち、最も多くの装置が共有するデバイス鍵を図7に示すテーブルから選択する。この操作を、無効化すべき装置を除く全ての装置が持つデバイス鍵が選択されるまで繰り返し行う。



#### [0049]

図11は、装置1を無効化する場合の、記録媒体に格納される鍵無効化データを示している。装置1を除く最大の部分集合は2345678であり、前記部分集合に割り当てられたデバイス鍵K28を用いて暗号化した暗号化メディア鍵が格納されている。さらに、暗号化メディア鍵と共に、暗号化に用いたデバイス鍵を特定するための部分集合に関する情報も合わせて格納する。

#### [0050]

図12は、記録装置110、並びに記録媒体120の構成要素を示している。記録装置110は、鍵管理装置100より発行されたデバイス鍵を格納するデバイス鍵格納部1201に格納するデバイス鍵と、記録媒体120に記録された鍵無効化データから復号鍵を選択/生成する復号鍵生成部1202と、鍵無効化データを復号鍵生成部1202で選択/生成した復号鍵で復号する復号部1203と、復号部1203で復号して得たメディア鍵でコンテンツ鍵を暗号化する暗号化部1204と、コンテンツ鍵でコンテンツを暗号化する暗号化部1205を備える。記録媒体120は、鍵管理装置100より発行された鍵無効化データを格納する鍵無効化データ格納部1011と、暗号化されたコンテンツ鍵を格納する暗号化コンテンツ鍵格納部1012と、暗号化されたコンテンツを格納する暗号化コンテンツ格納部1013を備える。

#### [0051]

例えば、記録装置110が装置3で、K13、K3、K24、K25の4つのデバイス 鍵を持つ場合、記録媒体に記録されている部分集合に関する情報2345678と、図8 に示すデバイス鍵(部分集合)の相互関係を示すテーブルを用いて、デバイス鍵K24を 選択し、選択したK24と、擬似乱数生成器を1回用いることにより、K28を生成して メディア鍵を復号する。

#### [0052]

図13は、記録装置110によりコンテンツが記録された記録媒体の例を示している。図14は、記録媒体120、並びに再生装置130の構成要素を示している。なお、記録媒体120の構成要素は図10と同様であるため、その説明は省略する。再生装置130は、鍵管理装置100より発行されたデバイス鍵を格納するデバイス鍵格納部1401と、デバイス鍵格納部1401に格納するデバイス鍵と、記録媒体120に記録された鍵無効化データから復号鍵を選択/生成する復号鍵生成部1402と、鍵無効化データを復号鍵生成部1402で生成した復号鍵で復号する復号部1403と、復号部1403で復号して得たメディア鍵で、記録媒体120から読み出した暗号化コンテンツ鍵を復号する復号部1405を備える。

#### [0053]

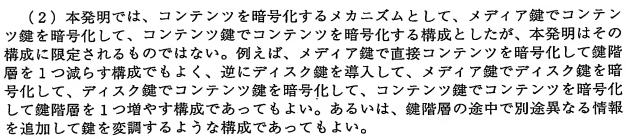
例えば、再生装置130が装置7で、K30、K20、K7、K8の4つのデバイス鍵を持つ場合、記録媒体に記録されている部分集合に関する情報2345678と、図8に示すデバイス鍵(部分集合)の相互関係を示すテーブルを用いて、デバイス鍵K20を選択し、選択したK20と、擬似乱数生成器を3回用いることにより、K28を生成してメディア鍵を復号する。

#### [0054]

(その他の変形例)

(1) 本発明では、記録媒体をDVD-RAMのようなレコーダプルメディアとする構成としたが、本発明はその構成に限定されるものではない。例えば、記録媒体をDVD-Videoのようなプリレコーディッドメディアとして、各再生装置がデバイス鍵を保有して、記録媒体に記録されたコンテンツを再生する構成であってもよい。また、この場合、記録媒体への書き込み装置がデバイス鍵を保有する必要はなく、鍵管理装置から直接メディア鍵を受け取り、そのメディア鍵に基づいてコンテンツを暗号化して書き込む構成であってもよい。

#### [0055]



#### [0056]

(3) 本発明では、鍵無効化データと暗号化コンテンツを同一の記録媒体に記録する構成としたが、本発明はその構成に限定されるものではない。例えば、鍵無効化データを記録する記録媒体と、暗号化コンテンツを記録する記録媒体を変えて配布する構成であってもよい。その場合、記録装置、あるいは再生装置では、まず、鍵無効化データが記録された記録媒体を挿入してメディア鍵を算出してから、別の記録媒体を挿入して、コンテンツの記録、あるいは再生を行う構成となる。

#### [0057]

- (4) 本発明では、鍵無効化データ、並びに暗号化コンテンツを記録媒体に記録して配布する構成としてが、本発明はその構成に限定されるものではない。例えば、放送や、インターネットなどの通信媒体を利用して配布する構成であってもよい。
- (5) 本発明では、鍵管理装置が、鍵、あるいは各装置を管理するための木構造を2分木として構成したが、本発明はその構成に限定されるものではない。例えば、木構造は3分木であっても、4分木であってもよい。

#### 【産業上の利用可能性】

#### [0058]

本発明にかかる鍵無効化システムは、各装置が保持する鍵に対して相互関係を持たせることにより、各装置が持つ鍵の数を削減することができるという効果を有し、同一システムにおいて、据え置き機や携帯端末などが混在する場合に、記憶容量の小さい携帯端末に対しては保持する鍵が少なくなるように割り当てることができるため、鍵無効化を実現するシステムにおいて有用である。

#### 【図面の簡単な説明】

#### [0059]

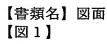
- 【図1】本発明に係る著作権保護システムの概念図
- 【図2】本発明に係る鍵管理装置の構成図
- 【図3】本発明に係る木構造の例を示す図
- 【図4】本発明に係るテーブル作成の動作フローを示す図
- 【図5】本発明に係る生成テーブルの例を示す図
- 【図6】本発明に係るデバイス鍵の割り当ての動作フローを示す図
- 【図7】本発明に係る生成テーブルの例を示す
- 【図8】本発明に係るデバイス鍵 (部分集合) の相互関係を示す図
- 【図9】本発明に係る各装置に対するデバイス鍵の割り当ての動作フローを示す図
- 【図10】本発明に係る各装置が保持するデバイス鍵の例を示す図
- 【図11】本発明に係る記録媒体に格納されるデータの例を示す図
- 【図12】本発明に係る記録装置、並びに記録媒体の構成図
- 【図13】本発明に係る記録媒体に格納されるデータの例を示す図
- 【図14】本発明に係る再生装置、並びに記録媒体の構成図
- 【図15】従来技技術の概念図
- 【図16】従来技術の木構造の例を示す図
- 【図17】従来技術の鍵生成の概念を示す図
- 【図18】従来技術の各装置に割り当てるデバイス鍵を示す図

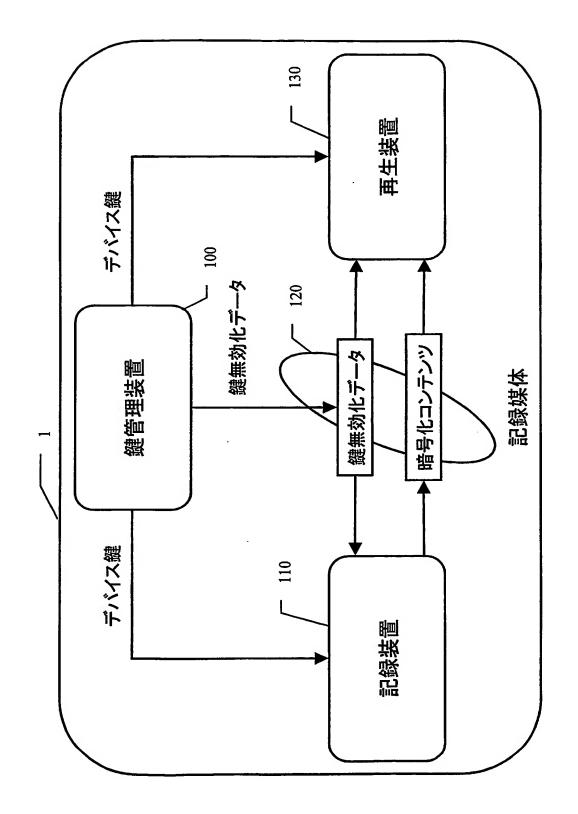
#### 【符号の説明】

[0060]

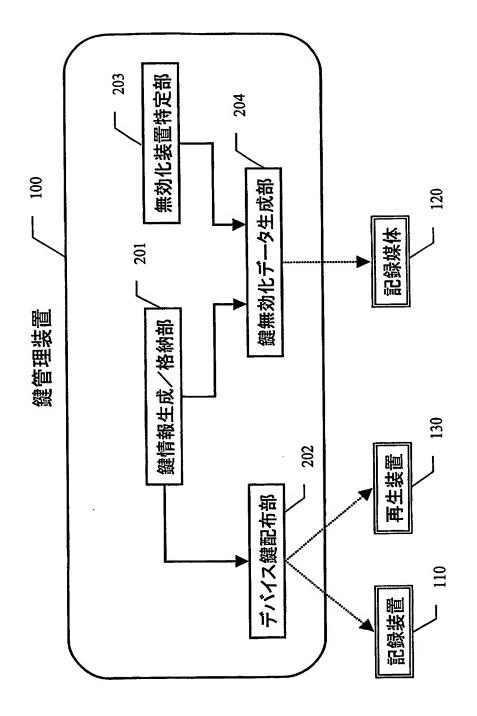


- 100 鍵管理装置
- 110 記録装置
- 120 記録媒体
- 130 再生装置
- 201 鍵情報生成/格納部
- 202 デバイス鍵配布部
- 203 無効化装置特定部
- 204 鍵無効化データ生成部
- 1011 鍵無効化データ格納部
- 1012 暗号化コンテンツ鍵格納部
- 1013 暗号化コンテンツ格納部
- 1201、1401 デバイス鍵格納部
- 1202、1402 復号鍵生成部
- 1203、1403、1404、1405 復号部
- 1204、1205 暗号化部

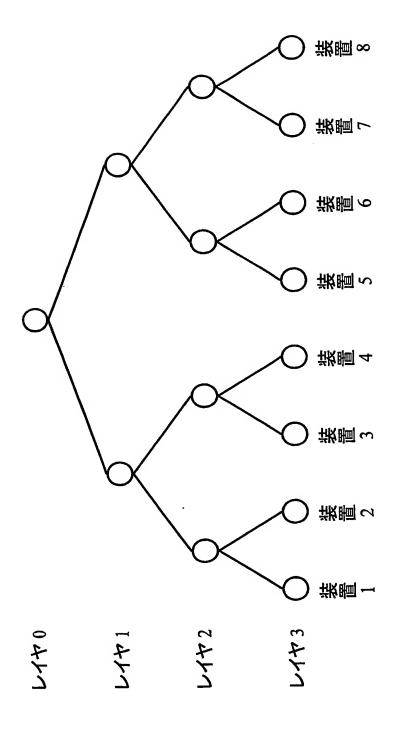


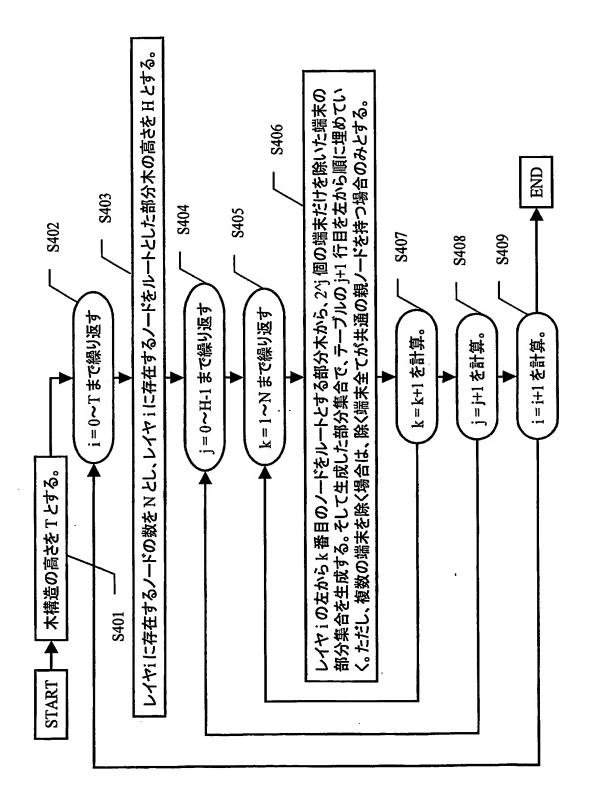






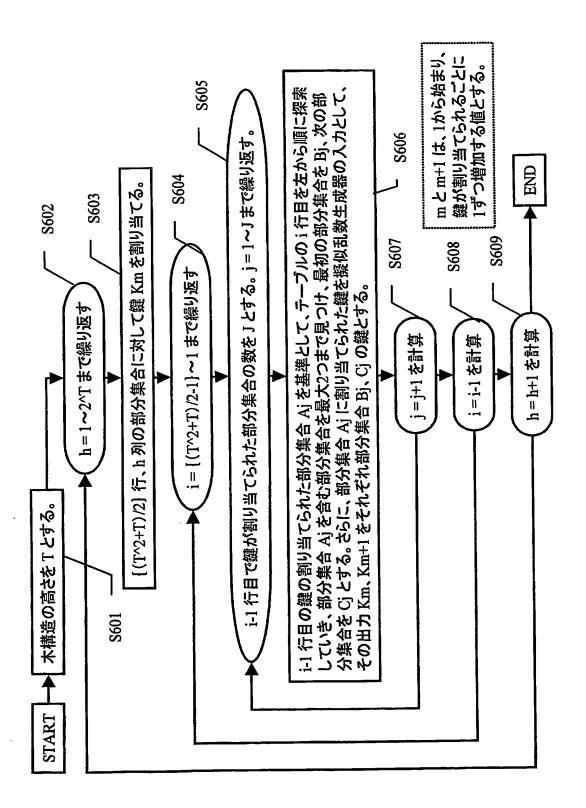








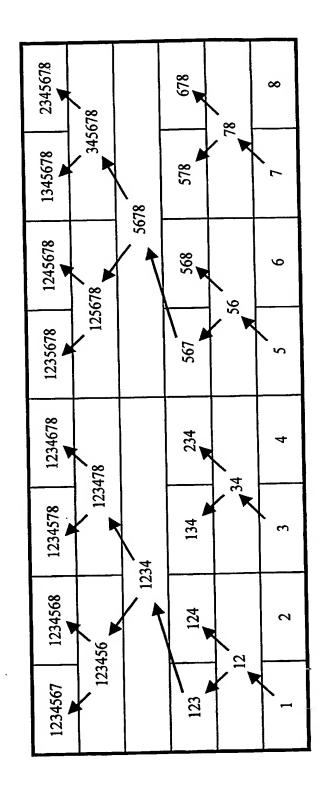
501	502	503				
	2345678			678		∞
	1345678			578		7
	1245678			268		9
	1235678			267		5
	1234786	345678		234	8.	4
	1234785	125678		134	95	3
	1234568	123478	8298	124	34	2
	1234567	123456	1234	123	12	1

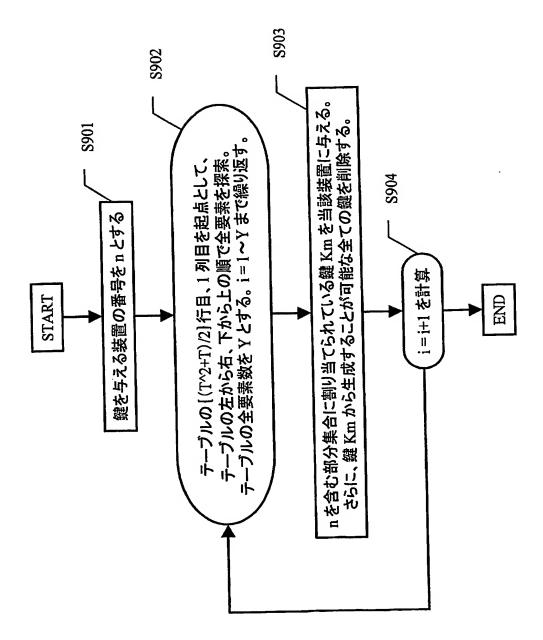




1234578	1234678	1235678	1245678	1345678	2345678
K10	K11	K25	K26	K27	K28
125678	345678				
K23	K24				
			• •		
134	234	267	268	578	829
K15	K16	K20	K21	K32	K33
95	78				
K19	K31				
3	4	5	9	7	∞
K13	K17	K18	K29	K30	K34





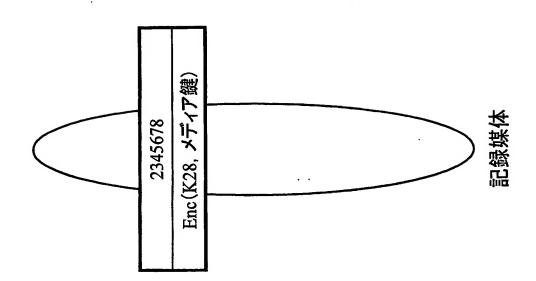




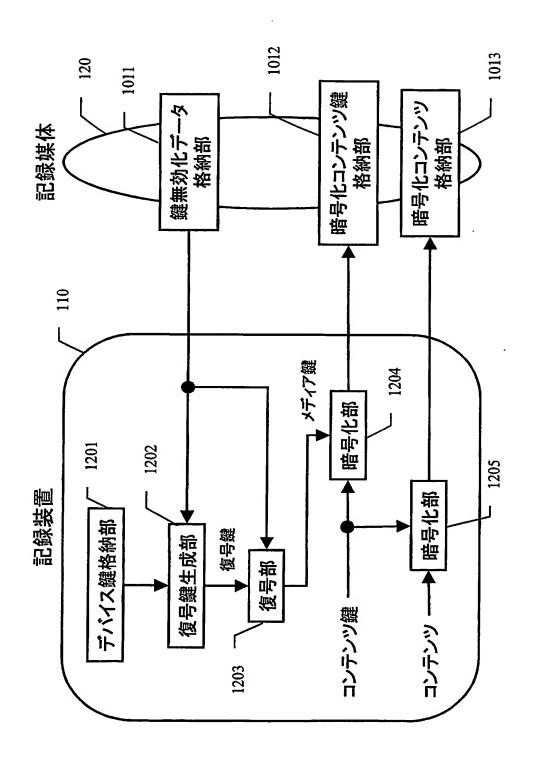
即共	1	134	125678	1345678		
※ 回	K1	K15	K23	K27		
Į.	2	12	234	125678	2345678	
光间2	K12	K2	K16	K23	K28	
Ť.	3	123	345678	1235678		
漫画	K13	K3	K24	K25		
į	4	34	124	1234	345678	1245678
<b>光直</b> 4	K17	K14	K4	KS	K24	K26
1	5	578	123456	1234578		
後回り	K18	K32	К6	K10		
III I	9	99	8/9	123456	1234678	
※回0	K29	K19	K33	К6	K33	
₹ <del>1</del> 2	7	292	123478	1234567		
	K30	K20	K7	K8		
B +	∞	78	568	123478	1234568	2678
※画8	K34	K31	K21	K7	K9	K22

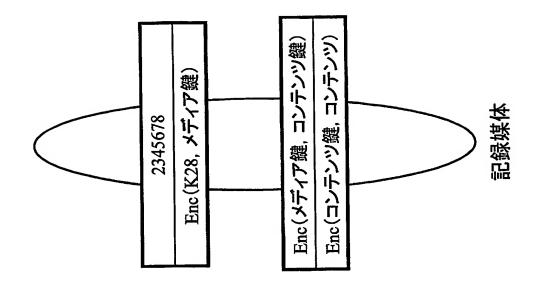


【図11】

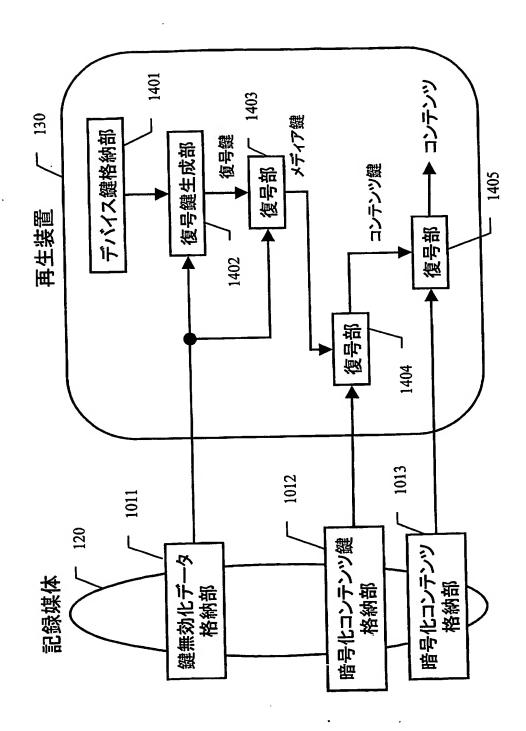






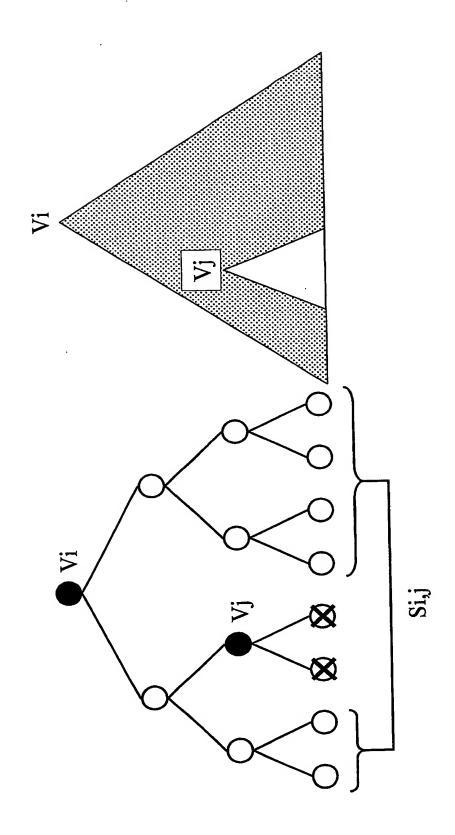


【図14】



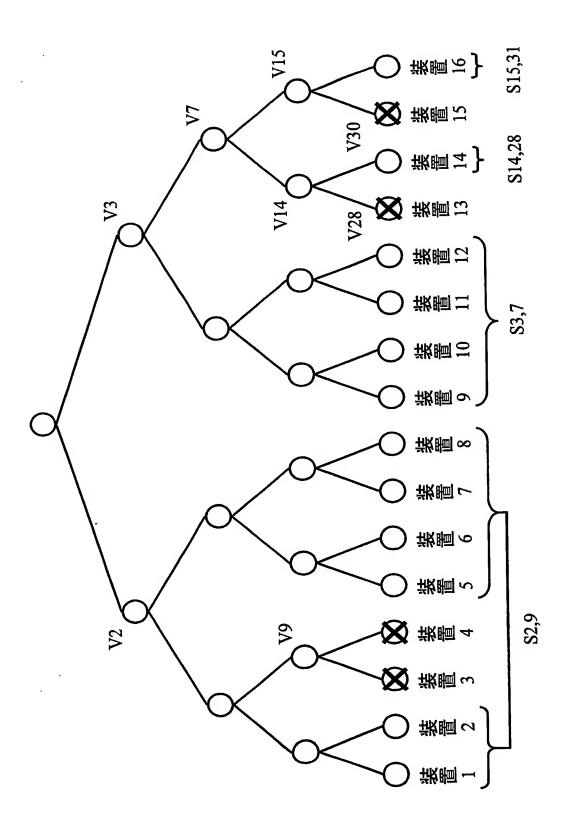


【図15】



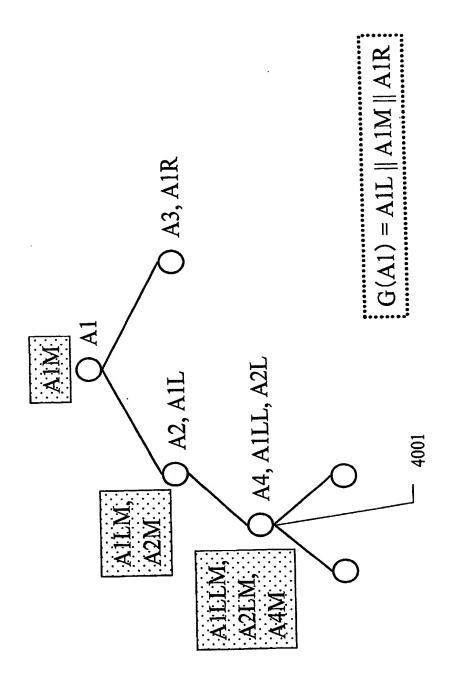


【図16】



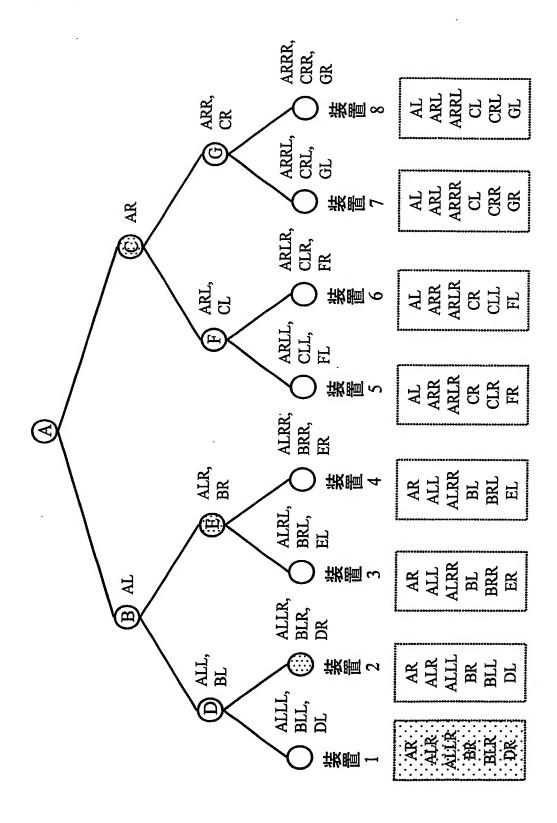


【図17】





【図18】





【書類名】要約書 【要約】

【課題】 従来の鍵無効化技術では、各装置が内蔵する鍵の数が膨大となる。

【解決手段】 鍵管理装置は、著作権保護システムに属する端末装置の部分集合を生成する部分集合生成部と、前記部分集合に対して鍵を割り当てる割当部と、前記部分集合が含まれる他の部分集合の鍵を前記割り当てた鍵から生成する鍵生成部と、前記部分集合に割り当てた鍵に基づいて無効化情報を生成する無効化情報生成部を備える。上記構成により、同一システムにおいて、据え置き機や携帯端末などが混在する場合に、記憶容量の小さい携帯端末に対しては保持する鍵が少なくなるように、各装置が保持する鍵に対して相互関係を持たせることにより、各装置が保持する鍵の数を削減する。

【選択図】 図1



特願2003-399968

出願人履歴情報

識別番号

[000005821]

1. 変更年月日 [変更理由] 住 所 氏 名 1990年 8月28日 新規登録 大阪府門真市大字門真1006番地 松下電器産業株式会社

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/017453

International filing date: 25 November 2004 (25.11.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP

Number: 2003-399968

Filing date: 28 November 2003 (28.11.2003)

Date of receipt at the International Bureau: 27 January 2005 (27.01.2005)

Remark: Priority document submitted or transmitted to the International Bureau in

compliance with Rule 17.1(a) or (b)



# This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record.

### **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

BLACK BORDERS
☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
☐ FADED TEXT OR DRAWING
☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
☐ SKEWED/SLANTED IMAGES
$\square$ COLOR OR BLACK AND WHITE PHOTOGRAPHS
☐ GRAY SCALE DOCUMENTS
LINES OR MARKS ON ORIGINAL DOCUMENT
REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
OTHER:

### IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.